54Mb Dual-Band Outdoor AP

Gemtek System P-780

User's Guide v1.2

Gemtek
s y s t e m s

Copyright

Notice

Trademarks

Within the 5.15 to 5.25 GHz band (5GHz radio channels 34 to 48) the U-NII devices are restricted to indoor operations to reduce any potential harmful interference to MSS operations.

FCC Warning

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Gemtek Systems declares that P-780 (FCC ID: MXF-AP931229AG) is limited in CH1~CH11 for 2.4GHz by specified firmware controlled in U.S.A

IC Warning

Operation is subject to the following two conditions:

- This device may not cause interference and
- This device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 8 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

Because high power radars are allocated as primary users (meaning they have priority) in 5250-5350 MHz, these radars could cause interference and/or damage to license exempt LAN devices.

Contents

About this Guide

Purpose

This document provides information and procedures on hardware installation, setup, configuration, and management of the Gemtek Systems high performance 54Mb Dual-Band Outdoor AP P-780.

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures. In addition, you should be familiar with the following:

- Hardware installers should have a working knowledge of basic electronics and mechanical assembly, and should understand related local building codes.
- Network administrators should have a solid understanding of software installation procedures for network operating systems under Microsoft Windows 95, 98, Millennium, 2000, NT, and Windows XP and general networking operations and troubleshooting knowledge.

Conventions Used in this Document

The following typographic conventions and symbols are used throughout this document:

⚠️	Very important information. Failure to observe this may result in damage.
❗	Important information that should be observed.
ℹ️	Additional information that may be helpful but which is not required.
bold	Menu commands, buttons and input fields are displayed in bold
`code`	File names, directory names, form names, and system-generated output such as error messages are displayed in constant-width type
`<value>`	Placeholder for certain values, e.g. user inputs
[value]	Input field format, limitations, and/or restrictions.

Help Us to Improve this Document!

If you should encounter mistakes in this document or want to provide comments to improve the manual please send e-mail directly to:

manuals@gemtek-systems.com

Gemtek Systems Technical Support

If you encounter problems when installing or using this product, please consult the Gemtek Systems website at www.gemtek-systems.com for:

- Direct contact to the Gemtek Systems support centers.
- Frequently Asked Questions (FAQ).
- Download area for the latest software, user documentation and product updates.

Chapter 1 – Introduction

Thank you for choosing the Gemtek Systems High Performance Dual-Band Outdoor Access Point P-780.

The Gemtek Systems P-780 operates simultaneously in the 5-GHz and 2.4-GHz frequency bands and is fully compliant to 802.11b/g and 802.11a standard with its high performance and enhanced security. P-780 is an important part for the Gemtek Systems HotZone solution as 11a/b/g outdoor AP.
The two Dual-Band radio (a/g + a/g) that this product provides supplies the furthest in flexibility and makes sure low interference and large coverage. The a+g operation mode and Multiple BSSID that this product provides differentiates it from traditional outdoor AP product.

Product Overview

Flexibility and high performance

The Gemtek Systems P-780 is a high performance outdoor AP for HotZone service. The two Dual-Band radios and AP/Bridge operation mode supply the furthest flexibility for wireless applications:

- Simultaneously supports 802.11a/b/g in one platform
- Mix AP and Bridge mode configuration work simultaneously, blanketing last mile with high-speed bandwidth
- Dual AP configuration for high client density environment
- Dual Bridge configuration for wireless repeating and wireless bridging areas

Secure and reliable wireless networking

The Gemtek Systems P-780 supplies multiple methods to protect the wireless network:

- Supports VLAN, up to 16 VLAN ID
- IEEE 802.1x/EAP with password, certificates and SIM card
- 64bits/128bits static and dynamic WEP key
- Supports Wi-Fi Protected Access(WPA)
- Layer 2 Isolation for preventing snooping under the same radio
- MAC ACL for preventing illegal attacking from Internet

Multiple BSSID

Supports up to16 BSSID, each of BSSID can be configured independently such as using different SSID, security, authentication method, and VLAN ID.

Management Option

You can use the Access Controller management systems through the following interfaces:

- Web-browser interface with HTTPS
- Command Line interface (CLI) with optional SSH
- Simple Network Management Protocol

P-780 management system pages are organized the same way for the web-browser interface and the CLI. This user manual provides detailed description of each management option.

Features Highlight

Super Brige

- 802.11a/b/g compliant
- 108Mbps raw data rate supporting
- Up to 20 bridge links supporting
- Special radio for Bridge
- WPA/PSK over Bridge link

Super AP

Multiple BSSID (up to 16)

- SSID per BSSID
- Enabled or Disabled Hidden SSID per BSSID
- VLAN ID per BSSID
- AAA way per BSSID, 802.1x and web login
- Co-existence of 802.1x and web login
- Security policy per BSSID
- WPA passthrough
- RADIUS server per BSSID

AAA

- RADIUS client supporting
- 802.1x supporting(EAP/TLS,EAP/TTLS, EAP/PEAP and EAP/SIM)

Security

- Static 64/128bits WEP, Dynamic 64/128bits WEP
- WPA/TKIP and WPA/AES support
- MAC ACL
- Access Control (accept rule and deny rule) based on MAC address
- Layer 2 Isolation
- Hidden SSID

Management

- Secure management via HTTPS, CLISH, SNMP
- Standard MIB and Gemtek Systems Private MIB
- Remote firmware update via WEB UI
- Backup/Restore configuration file
- DHCP Server

Chapter 2 - Installation

This chapter provides installation instructions for the hardware and software components of the Access Point P-780. It also includes the procedures for the following tasks:

- Hardware Introduction (LEDs, Connectors)
- Connecting the Access Point
- First Configuration

The Product Package

The product comes with the following:

- Dual-Band outdoor Access Point (model: P-780)
- Mounting Kit
- Screw Bag for Mounting Kit
- Waterproof tape
- Omni-directional antenna (A-807) * 2
- Installation CD containing:
    - P-780 User Guide in PDF format
    - KickStart Utility
    - Product Firmware
    - Release Notes
    - Adobe Acrobat Readers
    - Readme
- Printed 1 Year Warranty Card
- Printed Release Note
- Printed Warning Card

If any of these items are missing or damaged, please contact your reseller or Gemtek Systems sales representative.

A-807 antenna is the accessory of P-780 Product.

Refer to the Appendix D for A-807 Antenna Spec: D) Approved Antenna

The application example of waterproof tape can be referred to the Appendix E:

E) Waterproof Tape Application Example

Hardware Introduction

General Overview

Figure 1 – P-780 General View

The front panel of P-780 contains:

- There are 3 indicator lights (**LEDs**) that help to describe the state of various networking and connection operations.

The Bottom cover of P-780 contains:

- **Connectors** which enable you to make different network connections for the device
- **Reset** button enables you to reboot or reset the device configuration to the factory defaults

> Press the **Reset** button for less than **5** seconds to **reboot** the device.
>
> Press the **Reset** button for more than **5** seconds to **set** the device **to factory defaults**.

Bottom Cover
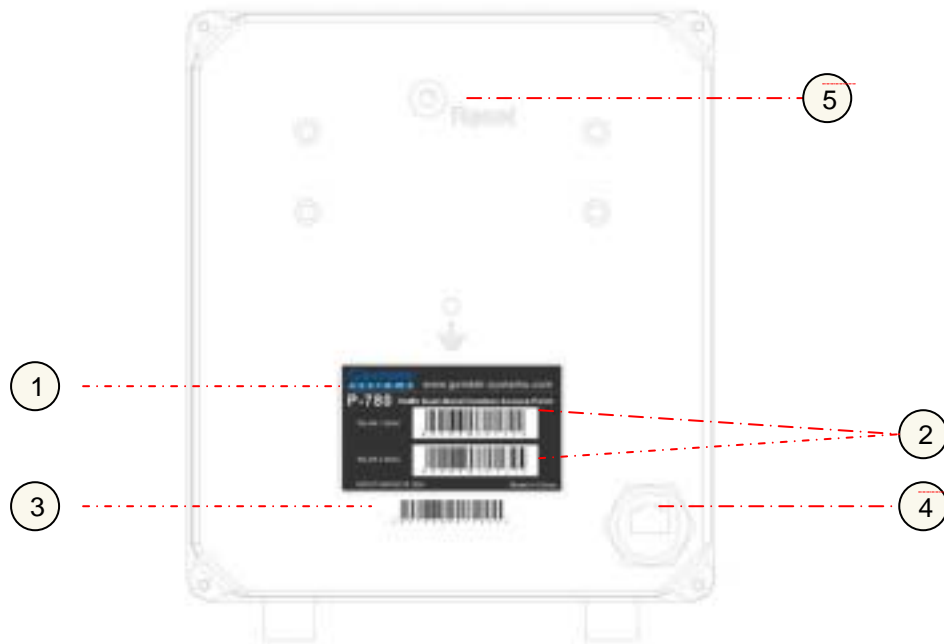
Figure 2 –Bottom Cover of the P-780

The Bottom Cover of the P-780 contains:

1. **Back Label** with Model and Device name. The official device name is **54Mb Dual-Band Outdoor Access Point**, model **P-780**.
2. **MAC address labels** of the device. The two labels show the **WLAN1** and **WLAN2** interface MAC address of the device.
3. **Serial Number label** of the device.
4. **LAN Port.** It is a waterproof RJ45 connector.
5. **RESET** Button**.** It is covered by a M5 Screw with a waterproof rubber washer

LEDs

The P-780 Access Point has 3 LEDs located on the front panel:
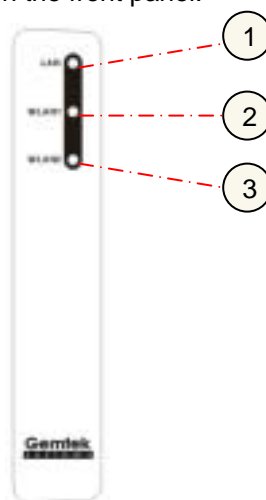
Figure 3 – LEDs of the P-780

The various states of the LEDs indicate different networking and connection operations as follows:

Item	LED	Color	Status	Indication
1	LAN	Green	On	P-780 Ethernet Port Link Active
			Blink	P-780 Ethernet Port is Transmitting and Receiving data
2	WLAN1	Green	On	P-780 WLAN1 RF card Active
			Blink	P-780 WLAN1 RF card is Transmitting and Receiving data
3	WLAN2	Green	On	P-780 WLAN2 RF card Active
			Blink	P-780 WLAN2 RF card is Transmitting and Receiving data

RF Connectors

The P-780 has 2 N-type RF connectors on the flank panel:

Figure 4 –RF Connectors

Descriptions of the connectors are given in the following table:

Item	Connector	Description
1	WLAN1	For WLAN1 RF card connecting to Antenna
2	WLAN2	For WLAN2 RF card connecting to Antenna

Hardware Installation

Installing the Access Point

Use the following procedure to prepare your network connection to P-780.

> **i** Use the enclosed POE and power cord or any others IEEE802.3af Compliant POE Power Source Devices to supply your P-780 Access Point.

Step 1   Assemble part 1 of the Mount Kit at the back of the bottom cover as shown in the following figure:
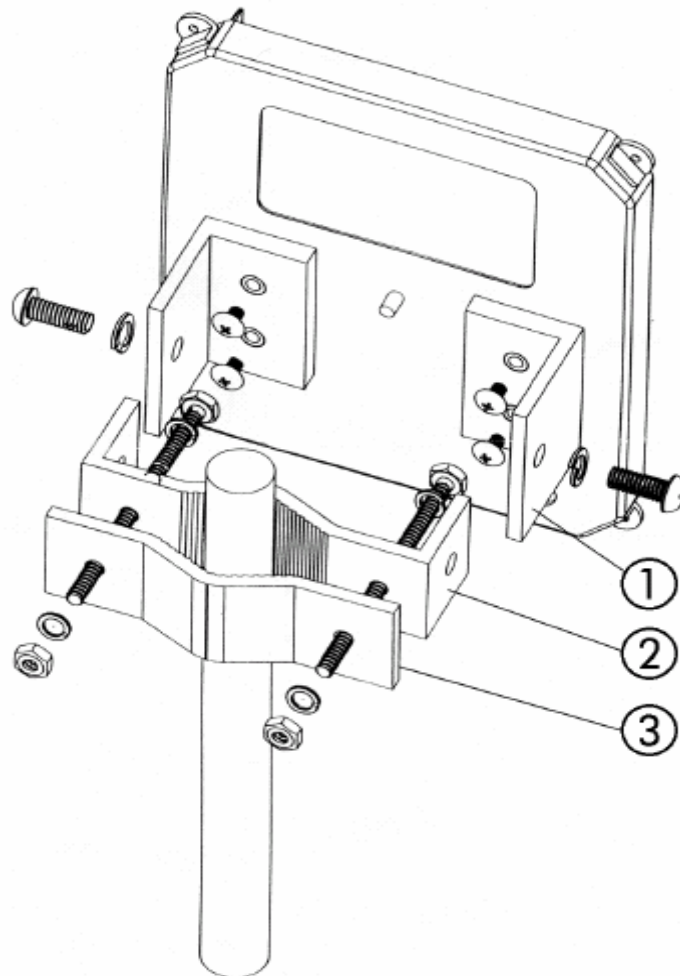
Figure 5 – Assembling the Mounting Kit to the P-780

Step 2   If you are mounting the AP on the wall, first install the bracket 2 of the mounting kit to a suitable position. Assemble the back of the P-780 case to the bracket ubsequently.
Step 3   If you are mounting the AP to a mast, first install the bracket 2 and the clip 3 of the Mounting to a mast. Assemble the back of the P-780 case to the bracket subsequently

Step 4   Assemble the one side of a Ethernet twist cable with the waterproof RJ45 connector .

⚠ !!!   Please read the description sheet in Waterproof RJ45 Connector package carefully
               before you do the assembly.

Step 5   Insert the the Ethernet twist cable to the LAN port connector on the back of the P-780
                Bottom Cover and screw down the nut.

Step 6   Connect two RF connectors to the Antennas by Jump RF cable with waterproof N-type
                plug.

Connect to the Power Source and Local Network

Step 1   Connect the Ethernet cable from the P-780 route to a IEEE802.3-2003 compliant Power
                source Equipment, Such as E-120 POE HUB,E-820 POE Switch from Gemtek Systems.

Step 2   If you use the E-120 POE HUB, please connect the P-780 LAN port to the

                PWR-LAN OUT port of E-120 and connect the E-120 **LAN-IN** port to the Switch or hub in
                the local network.

Figure 6 – Connecting P-780 to Power source and network by PoE HUB
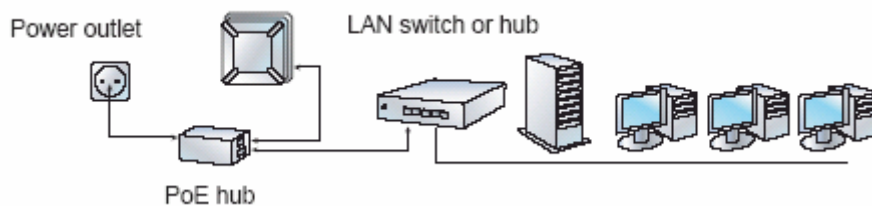
Software Installation

Initialization

There are two choices for the first web browser connection to your P-780: either enter the P-780's IP address and subnet (default networks settings) into the browser or launch the **KickStart** utility that is provided with your product CD.

The default network settings for your new access controller are:

```
LAN port:            IP 192.168.2.2        subnet 255.255.255.0
```

Software Introduction: KickStart

The Gemtek Systems **KickStart** is a software utility that is included on the Installation CD.

The utility automatically detects access points or access controllers installed on your network, regardless of its host IP address and lets you configure each unit's IP settings. The feature list for the **KickStart** utility is listed below:

- Scanning your subnet for all connected APs, ACs
- Quick access to your AP via HTTPS, telnet, SSH

To install the **KickStart** utility insert the Installation CD into your CD-ROM drive. Find and install the utility from the product CD into the computer.

> If the Installation CD does not start automatically, please run "**autorun.exe**" manually from the root directory of the installation CD.

Access Your P-780

There are two choices for the first Web browser connection to your P-780:

- Use the **Web browser**.
- Launch the **KickStart** utility that is provided with your product CD.

If first method is preferred follow these instructions:

Step 1   Configure your PC with a static IP address on the 192.168.2.0 subnet with mask 255.255.255.0. Connect the P-780 in to the same physical network as your PC. Open the Web browser and type the default IP address of the P-780:

```
https://192.168.2.2
```

Step 2   Enter the P-780 administrator login details to access the Web management.

> The default administrator log on settings for all access point interfaces are:
> User Name: **admin**
> Password: **admin01**

Step 3   After successful administrator log on you will see the main page of the P-780's **Web interface**:

If second method is prefered follow the instuctions:

Step 1   Install the **KickStart** utility from the **Installation CD**. Click **Start > Programs > Gemtek Systems > KickStart** to launch the application. If the P-780 device is connected to your network, the utility will automatically find your P-780:
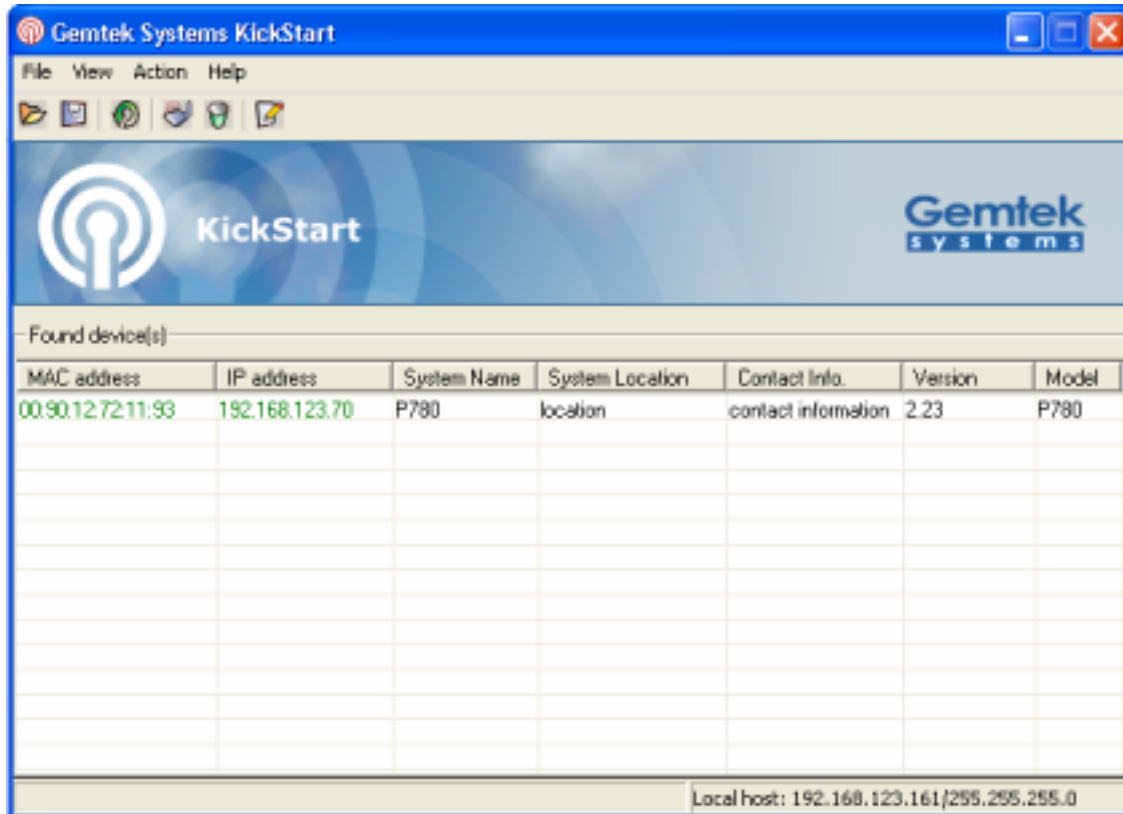
Step 2   Select your controller and right click. Select **Open WEB** item to launch the web
                    management interface through the secure https connection:
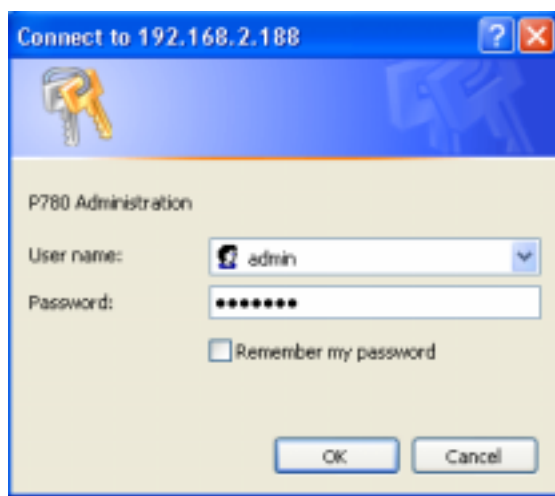
Step 3   Enter the P-780 administrator login settings to access the **web management** interface.

The default administrator log on settings for all access point interfaces are:
User name: **admin**
Password: **admin01**

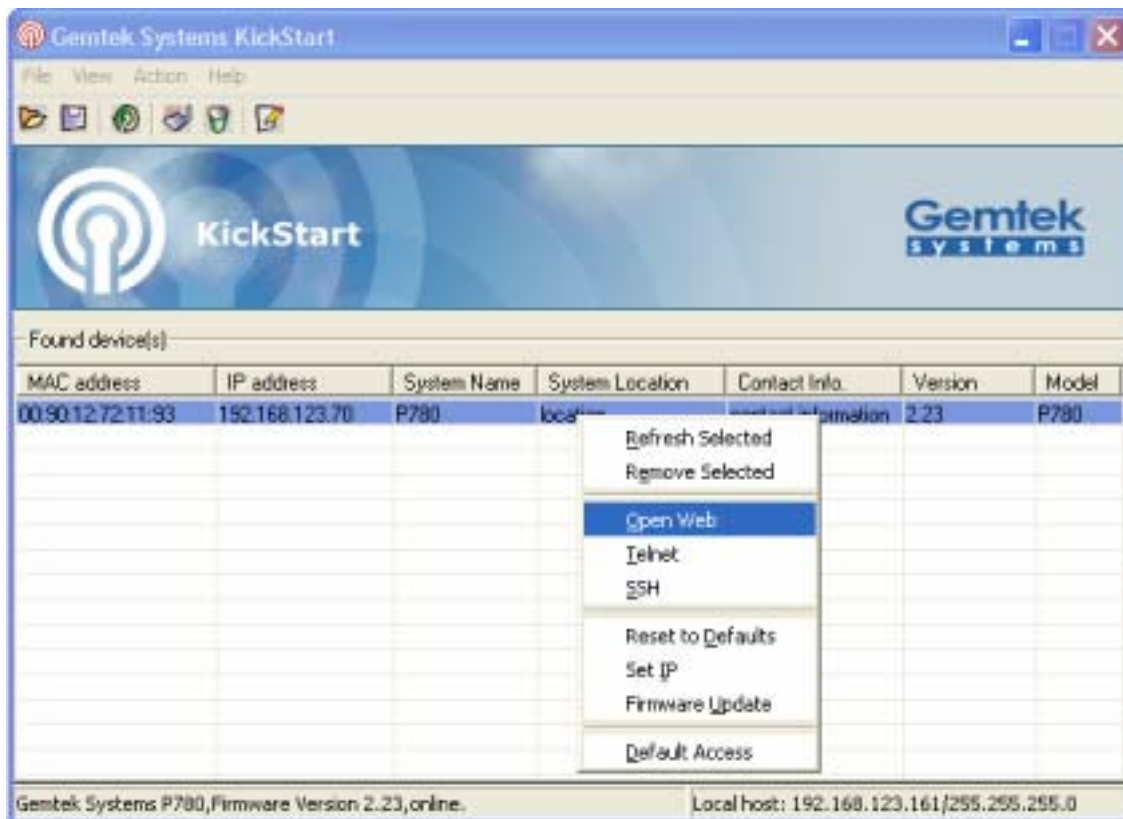**Step 4**   After successful administrator log on you will see the controller **web interface**.

P-780   EXIT

Status   Network   Wireless   System

Now you are enabled to perform your configuration.

Chapter 3 – Application Mode

The two Dual-Band chips (a/g + a/g) that this product provides supplies the furthest flexible application. Three application modes are supplied by P-780:

● AP + Bridge mode

● AP + AP mode

● Bridge + Bridge mode

AP + Bridge Mode

AP + Bridge configuration is for environment with last mile issue.

The typical usage is: 11g AP + 11a Bridge.
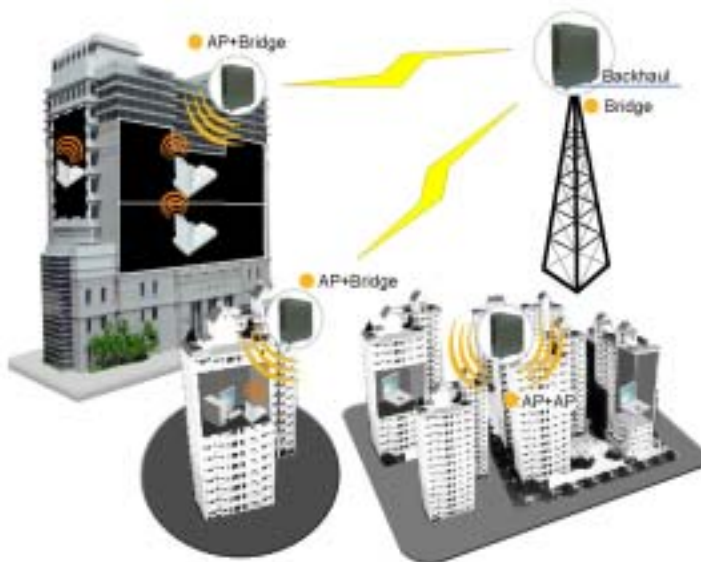
Figure 7 – AP +Bridge application mode

AP + AP Mode

AP + AP configuration can be for client density environment.

The typical usage is: 11g AP + 11a AP.

Figure 8 – AP +AP application mode

Bridge+ Bridge Mode

Bridge + Bridge mode is used in the area without Ethernet wiring.

The typical usage is: 11a Bridge + 11a Bridge for Point to Multi-Point or for wireless Repeater.
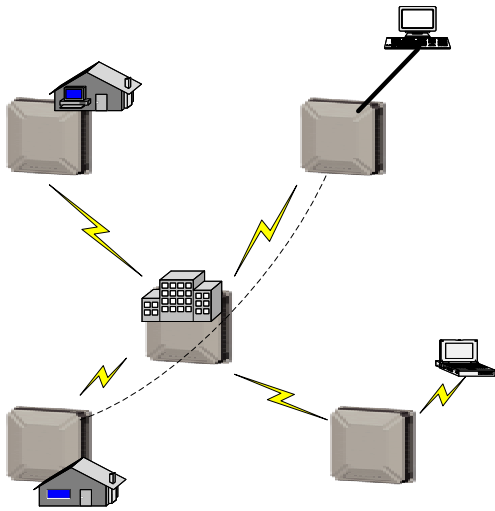
Figure 9 – Bridge +Bridge application mode in Point to Multi-Point

Figure 10– Bridge +Bridge application mode as wireless repeater

Chapter 4 – Reference Manual

This chapter contains web management reference information.

The **web management** main menu consists of the following sub menus:

- **Status** – device status showing
- **Network** – device settings affecting networking
- **Wireless** – device settings related to the wireless part of the P-780
- **System** – device system settings directly applicable to the P-780
- **Exit** – click exit and leave the web management then close your web-browser window.

Web Interface

The main **web management** menu is displayed at the top of the page after successfully logging into the system (see the figure below). From this menu all essential configuration pages are accessed.

Figure 11 – Main Configuration Management Menu

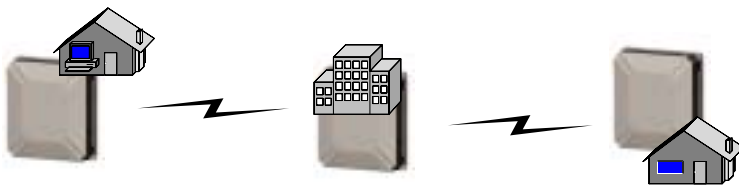The **web management** menu has the following structure:

Status

>   **Device Status** – show the status related with the whole device

>   **Wireless Status** – show the status of the two radios

Network

>   **Interface** – TCP/IP settings of P-780 LAN (Bridge) port

>   **RADIUS Server** – specify the settings of RADIUS server which is used by 802.1x or WPA

>   **DHCP Settings**– specify the settings of DHCP server or DHCP relay service

Wireless

>   **Basic** – specify the basic settings related with wireless part

>   **Advance** – specify the settings of multiple BSSID or Bridge

>   **WEP** – specify the WEP settings related with static WEP encryption

>   **MAC ACL** – MAC ACL settings for P-780

System

>   **Security** – set access permission to your P-780

>   **SNMP** – SNMP service

>   **Telnet** – Telnet/SSH service

>   **Configuration** – system configuration utilities, including Backup/Upload configuration

>   **Reset –** reboot device and restore systems to factory default

>   **Upgrade** – Upgrade the firmware remotely

In the following sections, short references for all menu items are presented.

Status

Status | Device Status

The device status page shows important information for the P-780, its system status and network configuration.

System	
System Version	P-780.GSI.2.24.2612
Uptime	7 day(s) 21:10
Wlan1 MAC	00:90:4b:d5:6f:6c
Wlan2 MAC	00:90:4b:d5:6f:7c
Free System Memory	34,748 K bytes
Total System Memory	63,368 K bytes

Network	
LAN Mode	static-IP
LAN IP	192.168.234.254
LAN Mask	255.255.255.0
Gateway	192.168.234.1

Note:

Figure 12 – Device Status

System Version display the current version of the firmware loaded to the AP

> This is important information for support requests and for preparing firmware upgrading

Uptime indicates the time, expressed in days, hours and minutes since the system was last rebooted.

Wlan1 MAC / Wlan 2 MAC shows the MAC addresses of the two wireless interfaces of the P-780

Free System Memory indicates the memory currently available in the P-780

Total System Memory indicates the total memory in the P-780

LAN Mode indicate static IP or DHCP client is used for P-780 LAN IP address

LAN IP shows the LAN IP address of P-780

LAN Mask shows the LAN Network Mask of P-780

Gateway shows the default gateway of P-780

Status | Wireless Status

The wireless status shows the information related with P-780 two wireless interfaces.

⊟ **Radio1**	
Channel	1
Domain	WORLD
Mode	AP
Band	2.4GHz(Mixed 11g)
Layer2 Isolation	disabled
Total Connected Clients	11
Antenna Gain	4dBi
Total Output Power(EIRP)	17dBm
MAC ACL	disabled

⊟ **Radio2**	
Channel	56
Domain	WORLD
Mode	AP
Band	5GHz(11a)
Layer2 Isolation	disabled
Total Connected Clients	0
Antenna Gain	7dBi
Total Output Power(EIRP)	17dBm
MAC ACL	disabled

Note:

Figure 13 – Wireless Status

Radio1 / Radio2 relates with two wireless interfaces

Channel indicates which channel is in use.

Domain indicates regulatory domain set on the P-780

Mode AP or Bridge mode is be used for this wireless interface

Band specify which band is in use for wireless interface

Layer2 Isolation specify the status of Layer2 Isolation service on this wireless interface

Total Connected Clients indicates number of the currently connected clients to your P-780

Antenna Gain indicates antenna Gain value. If use A-807, which is approved/attached Antenna of P-780, **Antenna Gain** shows 4dBi in 2.4GHz and 7dBi in 5GHz for regulation's limitation. If use other external antenna, this will shows 0dBi.

Total Output Power (EIRP) indicates EIRP value set to the P-780

MAC ACL indicates the status of MAC ACL feature on P-780

Network

Network | Interface

The interface configured is bridge device therefore only one interface is displayed here for configuration.

Bridge interface and its settings are listed in the **Interface** page.

⊟ **Network Interface Configuration**				
IP Address	Netmask	Gateway Address	Protocol	Action
192.168.2.2	255.255.255.0	0.0.0.0	static	Edit

Note:

Figure 14 – Interface Configuration Table

To change network interface (bridge) configuration properties click the **Edit** button in the **Action** column. The **status** can be changed now:

Figure 15 – Edit Interface Configuration Settings

IP Address - specify new interface IP address [in digits and dots notation, e.g. 192.168.123.70].

Netmask – specify the subnet mask [[0-255].[0-255].[0-255].[0-255]].These numbers are a binary mask of the IP address, which defines IP address order and the number of IP addresses in the subnet.

Gateway Address – interface gateway. For Bridge type interfaces, the gateway is always the gateway router.

Protocol – specify **static** for setting IP address manually and **dhcp** for getting IP address dynamically acting as DHCP client.

> When **dhcp** is used for getting IP address, Kickstart is recommended to find your device.

Save – save the entered values.

Cancel – restore all previous values.

Change status or leave in the default state if no editing is necessary and click the **Save** button.

Figure 16 – Apply or Discard Interface Configuration Changes

Apply Changes – to save all changes in the **interface** table at once.

Discard Changes – restore all previous values.

For such each change of settings, the P-780 needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Figure 17 – Reboot Server

Reboot – Click the button to restart the server and apply the changes.

[i] If there is no other setting needed to be modified, click the **Reboot** button for applying all modifications.

And if there are still other setting modifications needed, go ahead to finish all changes and then click **Reboot** button to restart and apply all settings together.

To reboot at once, click **Reboot** button and then it is necessary to wait a moment. And the message of reboot appears just like bellows:

Figure 18 – Reboot Information

Network | RADIUS Server

[i] Up to **32** different RADIUS servers can be configured under the **RADIUS servers** menu.

By default, one **RADIUS** server is specified for the system:
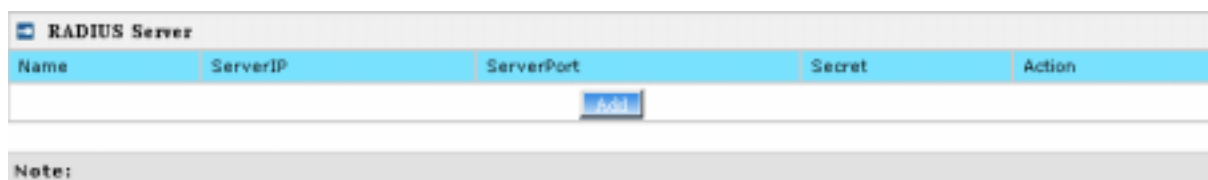

Figure 19 – RADIUS Servers Settings

Add – add new RADIUS server.

Click **Add** to configure RADIUS server settings.

Figure 20 – RADIUS Server's Details

Name – specify the new RADIUS server name which is used for selecting RADIUS server.

Server IP – authentication RADIUS server IP address [dots and digits].

Server Port – specify the network port used to communicate with RADIUS [1-65535].

> The port default value of 1812 is based on RFC 2138 "Remote Authentication Dial-in User Service (RADIUS)".

Secret – shared secret string that is used to make sure the integrity of data frames used for authentication server.

Save – add new specified RADIUS server.

Cancel – restore all previous values.

After adding a new RADIUS server or editing an existing one, the following control appears:

Edit – edit an existing RADIUS server settings

Delete – delete an existing RADIUS server settings

Reboot – restart the controller to make applied changes work.

> If there is no other setting needed to be modified, click the **Reboot** button for applying all modifications.
> And if there are still other setting modifications needed, go ahead to finish all changes and then click **Reboot** button to restart and apply all settings together.

Network | DHCP Settings

P-780 can act as DHCP server or DHCP relay. The DHCP (Dynamic Host Configuration Protocol) service is supported on physical interfaces.

DHCP server and DHCP relay is disabled by default.

Figure 21 –DHCP Settings

Edit – edit the wireless basic settings

To change DHCP setting properties click the **Edit** button, the DHCP server or DHCP relay service should be configured:

Figure 22 –DHCP Settings

Status – Select status from the drop-down menu.

>   **Disabled** – Disable the DHCP server service.

>   **DHCP Server** – Enable the DHCP server service.

>   **DHCP Relay** – Enable the DHCP Relay service.

Choose DHCP Server to enable DHCP server service. Choose DHCP Relay to enable DHCP relay service.

DHCP Server

This DHCP server service enables clients on the LAN to request configuration information, such as IP address, from a server. Settings of the DHCP service can be viewed just like the follow page.

Figure 23 –DHCP server Settings

> By default, DHCP server is disabled for P-780.

IP Address from / IP Address to – specify the IP address range to be dynamically allocated by the DHCP server.

Netmask – enter the netmask for IP pool range.

Gateway – enter the gateway IP for wireless clients.

WINS Address (Windows Internet Naming Service) – specify server IP address if it is available on the network [dots and digits].

Lease Time – specify the IP address lease interval in seconds [1-1000000].

Domain – specify the DHCP domain name [optional, 1-128 sting].

DNS address – specify the DNS server's IP address [in digits and dots notation].

DNS secondary address – specify the secondary DNS server's IP address [in digits and dots notation].

Change status or leave in the default state if no editing is necessary and click the **Save** button.

DHCP Settings	
Name	**Value**
Status	DHCP Server
IP Address from	192.168.123.2
IP Address to	192.168.123.254
Netmask	255.255.255.0
Gateway	192.168.123.1
WINS Address	0.0.0.0
lease time(seconds)	864000
Domain	
DNS Address	0.0.0.0
DNS Secondary Address	0.0.0.0
	Edit

Apply Changes   Discard Changes

Note:

Figure 24 –Apply or Discard DHCP server Settings

> The DHCP server settings will be automatically adjusted to match the network interface settings.

> The Gateway of DHCP server settings must be same with the Gateway of P-780

For each change of settings, the P-780 needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Figure 25 – Reboot information

Reboot – Click the button to restart the server and apply the changes.

> If there is no other setting needed to be modified, click the **Reboot** button for applying all modifications.
> And if there are still other setting modifications needed, go ahead to finish all changes and then click **Reboot** button to restart and apply all settings together.

> When P-780 network Interface uses DHCP to get IP address dynamically, DHCP server service cannot be enabled.

When P-780 uses DHCP to get IP address, the similar WEB UI will be appears:

Figure 26 – Warning information

DHCP Relay

To route DHCP through the external server, enable the **DHCP Relay** service.

DHCP Settings	
Name	Value
Status	DHCP Relay ⌄
Server IP	192.168.2.1
	Save Cancel

Note:

Figure 27 – DHCP Relay settings

Server IP: enter the IP address of the external DHCP server.

Change status or leave in the default state if no editing is necessary and click the **Save** button.

DHCP Settings	
Name	Value
Status	DHCP Relay
Server IP	192.168.2.1
	Edit

Apply Changes   Discard Changes

Note:

Figure 28 –Apply or Discard DHCP relay Settings

For each change of settings, the P-780 needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

DHCP Settings	
Name	Value
Status	DHCP Relay
Server IP	192.168.2.1
	Edit

Note:

Reboot

Server needs to be restarted. Please reboot.

Figure 29 – Reboot information

Reboot – Click the button to restart the server and apply the changes.

If there is no other setting needed to be modified, click the **Reboot** button for applying all modifications.
And if there are still other setting modifications needed, go ahead to finish all changes and then click **Reboot** button to restart and apply all settings together.

Wireless

Wireless | Basic

Use the **wireless | Basic** menu to configure such wireless settings as regulatory domain, channel, band, and power, layer2isolation. Click the edit button on the setting you need to change:

Figure 30 – Basic Wireless Settings

Site Survey –perform survey to show overview information for wireless networks in a local geography

The site survey shows overview information for wireless networks in a local geographic area. Using this survey, administrator can scan for working access points, check their operating channels, and see RSSI levels. To start the scan, simply click the **Site Survey** menu.

After clicking **Site Survey**, you will get the follow warning:

Figure 31 – Site Survey warning

Click OK to continue site survey and get the similar UI:

Figure 32 – Site Survey information

To refresh the statistics click the **Rescan** button.

During Site Survey, all wireless clients which are connecting with P-780 would be kicked off.

Site Survey takes some minutes to perform. Please wait and don't power off AP during site survey.

Edit – edit the wireless basic settings

To change basic wireless setting properties click the **Edit** button in the **Action** column. The **status** can be changed now:

Figure 33 – Edit Basic Wireless Settings

Change status or leave in the default state if no editing is necessary and click the **Save** button.

Figure 34 – Apply or Discard Basic Wireless Settings

Radio – specify which wireless interface of P-780 is shown

Domain – select the regulatory domain according to your country

The full frequency range of the 2.4 GHz or 5 GHz is not permitted for use in all countries. Depending on your selection of regulatory domains, the available frequency channels will vary.

Before changing radio settings manually verify that your settings comply with government regulations. At all times, it will be the responsibility of the end-user to ensure that the installation complies with local radio regulations. Refer to the Appendix:
C) Regulatory Domain/Channels**.**

Channels – select the channel that the access point will use to transmit and receive information. If one channel is defined, it acts as default channel. Channels list will vary depending on selected regulatory domain and selected band. Multiple frequency channels are used to avoid interference between two radios of this AP, and between nearby access points. If you wish to operate more than one access point in overlapping coverage areas, we recommend a distance of at least four channels between the chosen channels. For example, for three Access Points in close proximity choose channels 1, 6 and 11 for 11b/g or channels 36, 40 and 64 for 11a.

Band – working bands on which your radios are working.

Antenna Gain: When using the approved antenna supplied by Gemtek System, you must select the Antenna A-807 in **Antenna** item to meet the regulation's power limitation. A-807 is 4.5dBi in 2.4GHz, 5dBi in 5GHz.

A-807 antenna is the accessory of P-780 Product.

RTS Threshold – when set, this settings specifies the maximum packet size beyond which RTS/CTS mechanism is be invokes. The value range of this is [0 …2347]. Default is 2346 which means that RTS is disabled.

Layer 2 Isolation – Layer2 wireless client separation. Connected clients with user isolation function enabled cannot access each other directly. The clients are isolated from each other using their MAC addresses [enabled/disabled].

Mode – two modes are supplied: AP mode and Bridge mode.

For such each change of settings, the P-780 needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Basic Wireless Setting	
Radio :	wlan1
Name	**Value**
Domain	WORLD
Channel	11
Band	2.4GHz(Mixed 11g)
Total Output Power (EIRP)	14dBm
Antenna Gain	4dBi
RTS Threshold	2347 bytes
Layer2 Isolation	disabled
Mode	AP
Action	Edit Site Survey

Note:
Reboot
Server needs to be restarted. Please reboot.

Figure 35 – Reboot Server

Reboot – Click the button to restart the server and apply the changes.

If there is no other setting needed to be modified, click the **Reboot** button for applying all modifications.
And if there are still other setting modifications needed, go ahead to finish all changes and then click **Reboot** button to restart and apply all settings together.

Wireless | Advance

P-780 supports **Multiple BSSID (MBSSID)** function. You can configure up to 16 BSSIDs per radio on P-780 and assign different configuration settings to each BSSID. For wireless users, they can think P-780 as single AP with multi service supporting, including different security policy, different VLAN ID, different authentication etc. All the BSSIDs are active at the same time that means client devices can associate to the access point for specific service. Use the **Wireless | Advance** menu to configure properties related to Multiple BSSID, including configure SSID, Hidden SSID, VLAN, and Security for each SSID.

> Each BSSID can have its own SSID, In this case, Multiple BSSID is the same with Multiple ESSID. Wireless users can think P-780 as multiple virtual APs, each supporting different service, and connects one SSID for the special services.

Also, P-780 supports **Bridge** function, it can support up to 20 **Bridge links** per radio. Different bridge link can use different WEP key index.

AP Mode:

Figure 36 – Advanced Wireless Setting (AP Mode)

Radio – specify which RF card (wlan1 or wlan2) is needed to be configured since P-780 has two Dual-Band radios

Mode – specify the operation mode of P-780 (AP or Bridge)

Interface – Choose the specified **MBSSID** entry you want to configure. Each Interface maps to a BSSID

Hidden – Show the status of Hidden SSID feature

Security – Show which security policy is used for this **MBSSID** entry

Current Connect # – Show the number of current wireless clients who are connecting with this MBSSID

New – Create a new **MBSSID** entry

Detail – Show the detail information of this **MBSSID** entry

Edit – Edit the selected **MBSSID** entry you want to configure

Delete – Delete the selected **MBSSID** entry. When in AP mode, you can not delete the last entry

Clicking Detail, a similar page will be appears as below:

Figure 37 – Detail for MBSSID entry

Detail – Show the MAC address of current connected clients

Return – Return to the wireless advance settings page

Clicking **New** or **Edit** on AP mode, the settings of MBSSID entry appears:

Figure 38 – Multiple BSSID Setting

Radio – showing which RF card (wlan1 or wlan2) is being configured.

Mode – showing the current operation mode of P-780 (AP or Bridge).

Interface – showing the current **MBSSID** | **Bridge link** entry

SSID – a unique ID for your wireless network. It is case sensitive and must not exceed 32 characters. The default SSID is "P-780" but you should change this to a personal wireless network name. The SSID is important for clients when connecting to the access point. All client stations must have their client SSID settings configured and must use the same SSID.

> Each MBSSID entry (BSSID) can has its own SSID. And SSID can be same for different BSSID

Hidden SSID – When enabled, the SSID of this Interface is invisible in the networks list while scanning the available networks for wireless client (SSID is not broadcasted with its Beacons). When disabled, the AP's SSID is visible in the available network list [enabled/disabled]. By default the Hidden SSID is disabled.

Use VLAN – When enabled, the outgoing packets from this SSID device will be tagged with VLAN ID and 802.1p tag (If have).

VLAN ID – Configure VLAN ID for each Multiple SSID devices. Valid numbers are from 1 to 4094.

802.1p Tag – Configure 802.1p Tag for remote APC's or Router's QoS uses. Valid numbers are from 0 to 7.

> VLAN ID and 802.1p tag must cooperate with remote Router or APC.

Security – Specify the security policy.

WEP – When selected, the privacy of MSSID entry will be set to WEP (Wired Equivalent Privacy).

WEP Key Index – Select the default key Index to make it the Default key and encrypt the data before being transmitted. All stations, including this MSSID Entry, always transmit data encrypted using this Default Key. The key number (1,2,3,4) is also transmitted. The receiving station will use the key number to determine which key to use for decryption. If the key value does not match with the transmitting station, the decryption will fail. The key value is set in **Wireless | WEP** web page.

802.1x – When selected, the MSSID entry will be configured as an 802.1x authenticator. It supports multiple authentication types based on EAP (Extensible Authentication Protocol) like EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM. The privacy will be configured as dynamic WEP.

RADIUS Server Profile – Select the default radius server name. If not, please configure Network | RADIUS Servers Web page first.

Dynamic Key Length – Select the dynamic 64-bits / 128-bits encryption.

WPA – Wi-Fi Protected Access, When selected, the encrypt method will be WPA with RADIUS Sever.

RADIUS Server Profile – The same as **802.1x**.

Algorithm – Choose WPA algorithm (TKIP, AES).

Use ReKey – If not selected, indicates that Group Key will not be rekeyed. If selected, must specify the time in minutes, after which the group key will be updated.

Every … minutes – Specify amount of minutes and WPA automatically will generate a new Group Key.

WPA-PSK – When selected, the encrypt method will be WPA without RADIUS Server.

Use Pre-Shared Key – Specify more than 8 characters and less than 64 characters for WPA with pre-shared key encryption.

Algorithm – The same as **WPA**.

Use Rekey – The same as **WPA**.

Every … minutes – The same as **WPA**.

MAC Auth – MAC authentication. When selected, the MAC address of username and password will be passed to RADIUS server for PAP authentication when wireless client connects with P-780.

RADIUS Server Profile – The same as **802.1x**.

Disabled – When selected, you don't select any security policy.

Bridge Mode
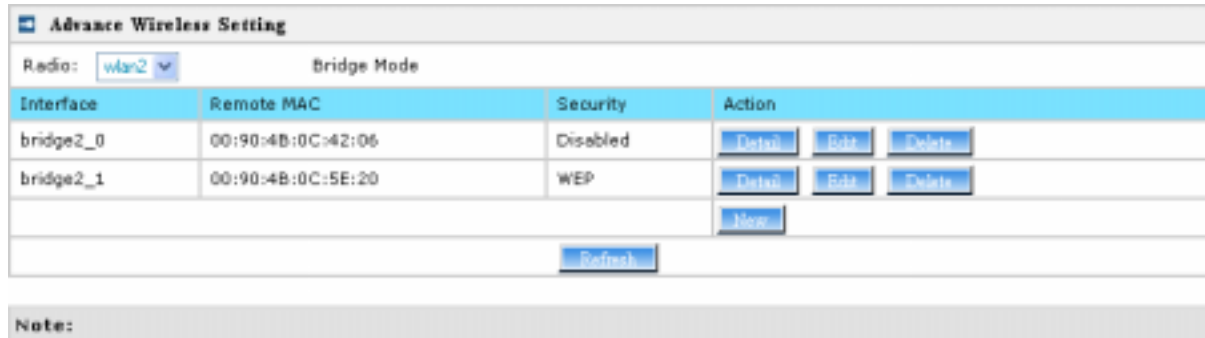
Figure 39 – Advanced Wireless Setting (Bridge Mode)

Radio – specify which RF card (wlan1 or wlan2) is needed to be configured since P-780 has two Dual-Band radios

Mode – specify the operation mode of P-780 (AP or Bridge)

Interface – Choose the specified **Bridge link** entry you want to configure.

Remote MAC – Specify the remote peer's MAC address of this Bridge

Security – Specify which security policy is used

New – Create a new **Bridge link** entry

Detail – Show the detail information of this **Bridge link** entry

Edit – Edit the selected **Bridge link** entry you want to configure

Delete – Delete the selected **Bridge link** entry.

Clicking **Detail**, the similar page will be appears:

Figure 40 – Detail of one bridge entry

Clicking **Edit** for editing an existed bridge link or **New** for adding a new bridge link, you can see the figure like this.

Figure 41 – Bridge Link Setting

Remote MAC – Add the remote peer's MAC address you want to configure as a bridge link

Security – Specify WEP or WPA-PSK (TKIP or AES) is used for security policy. WPA-PSK or static WEP can be used for encrypt each bridge link

Each Bridge link can have its own WEP key/keyIndex for encryption.
Only WEP can be used as security policy for Bridge links now. More enhanced security policy is in developing.
By default, four WEP keys are all set to "aaaaa". They can be modified in **Wireless | WEP**.

Wireless | WEP

Use the **Wireless | WEP** menu to configure static WEP settings.

This menu only set static WEP key value related with 4 key indexes for each RF card (wlan1 or wlan2). Enable or Disable static WEP is in the **Wireless | Advance** menu.

Figure 42 – WEP Settings

Radio – specify which RF card (wlan1 or wlan2) is needed to be set.

Click **Edit** to edit the existing **wepkey1** to **wepkey4**.

> By default, four WEP keys are all set to "aaaaa". They can be modified according to real need.

Figure 43 – Edit WEP Key

Wireless | MAC ACL

Use the **MAC ACL** service to control the default access to the wireless interface of the P-780 or define special access rules for mobile clients. Configure the ACL using the Wireless | MAC ACL menu:

Figure 44 – MAC ACL Service

Radio – Two wireless interfaces wlan1 and wlan2 can be selected for each radio's MAC ACL rules.

> Only AP mode has the MAC ACL service. The wireless interface whose mode is Bridge hasn't MAC ACL settings.

Policy Setting – click the **edit** button to choose Allow, Deny or disable the access control service on device. By default the ACL service is disabled and all wireless clients connecting to the P-780 are allowed (no ACL rules are applied to the wireless clients).

Select **Allow** means only the wireless clients whose MAC are listed in the **MAC List** would be permitted to access this AP. Other wireless client cannot access this AP.

Select **Deny** means only the wireless clients whose MAC are listed in the **MAC List** would be prevented from accessing. Other wireless clients can access this AP.

Select **Disabled** means no ACL service.

Figure 45 – MAC ACL settings

You must create **MAC List** to work with **Policy** setting. The access control list is based on the network device's MAC address. In the MAC ACL Configuration table, you only need to specify the MAC address of wireless client. Click the Add button to create a new MAC entry:

Figure 46 – Add MAC entry

MAC Address – enter the physical address of the network device you need to (MAC address) The format is a list of colon separated hexadecimal numbers (for example: 00:AA:A2:5C:89:56).

Save – click the button to save the new MAC entry.

Figure 47 – Apply or Discard MAC ACL Configuration Changes

Apply Changes – to save all changes made in the **interface** table at once.

Discard Changes – restore all previous values.

For such each change of settings, the P-780 needs to be restarted to apply all settings changes when clicking **Apply Changes**. Request for reboot server appears:

Radio Setting

Radio:	wlan1 ∨

Policy Setting

Policy	deny	Edit

MAC ACL Configuration

MAC List	Action
00:90:4B:00:02:19	Delete
Add	

Note:
Reboot

Server needs to be restarted. Please reboot.

Figure 48 – Reboot Server

Reboot – Click the button to restart the server and apply the changes.

> If there is no other setting needed to be modified, click the **Reboot** button for applying all modifications.
>
> And if there are still other setting modifications needed, go ahead to finish all changes and then click **Reboot** button to restart and apply all settings together.

System

System | Security

Use the **System | Security** service to configure the name and password administrator:

administrator	
UserName	admin
Old Password	
New Password	
Confirm Password	
	Save Cancel

Note: Administrator Password Setting

Figure 49 – system security settings

User Name – administrator username for access to P-780 (e.g. web interface, CLI mode) [1-32 symbols, spaces not allowed].

Old Password – old password value.

New Password –new password value used for user authentication in the system [4-8 characters, spaces not allowed].

Confirm Password – re-enter the new password to verify its accuracy.

Save – click to save new administrator settings.

> Default administrator logon settings are:
> User Name: **admin**
> Password: **admin01**

> Password length is from 4 to 8 characters.

System | SNMP

SNMP is the standard protocol that regulates network management over the Internet. To communicate with SNMP manager you must set up the same **SNMP** communities and identifiers on both ends: manager and agent.

Use the **System | SNMP** menu to change current SNMP configuration.

Figure 50 – SNMP settings

Readonly community – Community name is used in SNMP version 1 and version 2c. Read-only (public) community allows reading values, but denies any attempt to change values [1-32 all ASCII printable characters, no spaces].

Readwrite community – Community name is used in SNMP version 1 and version 2c. Read-write (private) community allows to read and (where possible) change values [1-32 all ASCII printable characters, no spaces].

Default Trap community – The default SNMP community name used for traps without specified communities. The default community by most systems is "public". The community string must match the community string used by the SNMP network management system (NMS) [1-32 all ASCII printable characters, no spaces].

Trap Configuration Table:

You can configure your SNMP agent to send **SNMP Traps** (and/or inform notifications) under the defined host (SNMP manager) and community name (optional).

Figure 51 – SNMP Trap table settings

Click **Add** to add a new SNMP manager or **Delete** to delete a specific SNMP manager. Clicking **Add**:

Figure 52 – Add SNMP Trap

Host IP – enter SNMP manager IP address [dots and digits].

Host Port – enter the port number the trap messages should be send through [number].

Trap Type – select trap message type [v1/v2/inform].

Community – specify the community name at a SNMP trap message. This community will be used in trap messages to authenticate the SNMP manager. If not defined, the default trap community name will be used (specified in the SNMP table) [1-32 all ASCII printable characters, no spaces].

Save – save all current settings

Cancel – restore the last settings

System | Telnet

Use **System | Telnet** menu to manage the telnet/SSH service of your P-780.

Figure 53 – System Configuration settings

Telnet Service – Enable or disable telnet service of P-780

SSH Service – Enable or disable SSH service of P-780.

The default of these two services are all **Enabled**. The current IETF SSH (SSHv2) is supported for security of accessing P-780 via telnet/CLISH.

System | Configuration

Use the **System | Configuration** menu to configure such system utilities:

- **Backup** – download current working system configuration for backup
- **Upload/Restore** – upload system configuration for restore

Figure 54 – System Configuration settings

You can save your current device configuration file locally using the **Backup** menu under the **System | Configuration | Backup** menu:

Figure 55 – Backup settings

Such device configuration is saved in the specific format file (.cfg).

Description Message shows the current version of firmware.

Click the **Preparation** button to start saving the configuration file.

Click the **Download** button to download current working configuration into your local PC.

Figure 56 – Download system configuration

You can upload saved configuration file any time you want to restore this configuration to the device by using the **Browse** button Select the configuration file and upload it on the device:
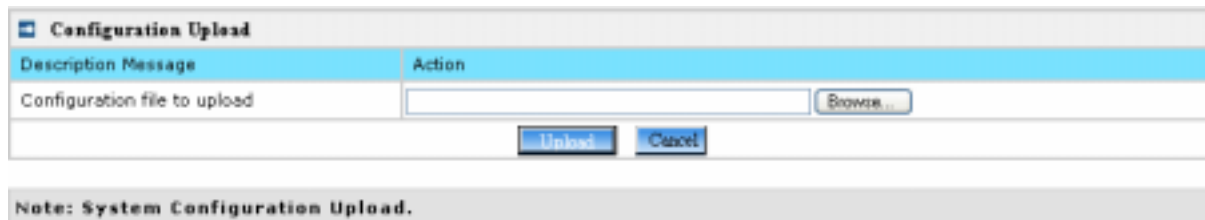
Figure 57 – Configuration Upload/Restore

Click **Upload** for upload the specified configuration and then the similar UI appears
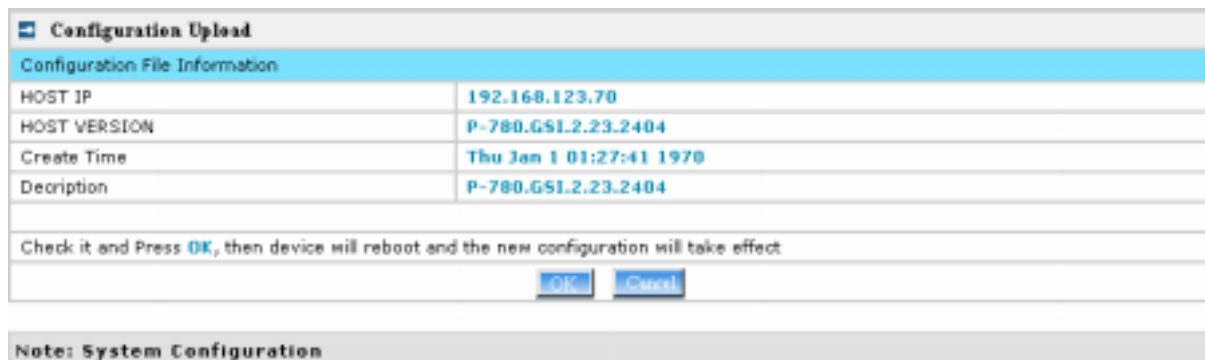
Figure 58 – configuration information

HOST IP – show the IP address in the configuration file that needs to upload.

> Please remember this IP address for accessing P-780 after the configuration file is uploaded.

HOST VERSION – show the firmware version in the configuration file that needs to upload.

OK – click the button to apply configuration setting to the device.

If everything is right, click **OK** button for upload/restore.

System | Reset

System Reset	
Description	**Action**
Current software version: P-780.GSI.2.11.0020(alpha)	
Reboot device	Reboot
Restore the original configuration from factory.	Reset

Note: System Reboot. System Reset.
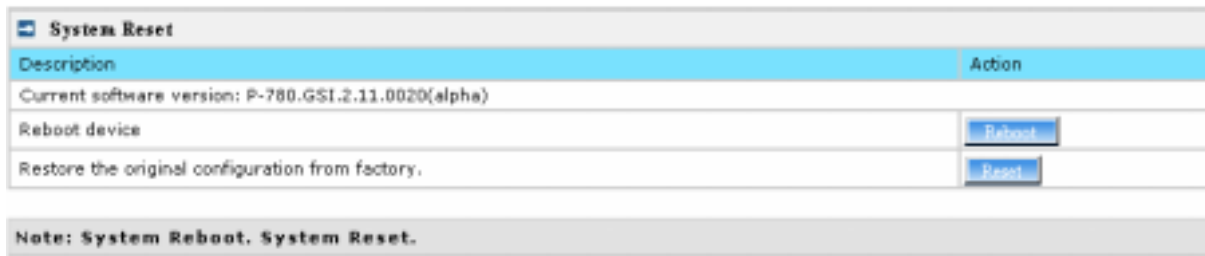
Figure 59 – System Reset setting

Reboot – Reboot the device

Reset – Reset System to Factory Defaults

To reboot the device, click **Reboot** and then the below appears to make sure:

System Reset	
Description	**Action**
Are you sure you want to REBOOT the device? It will take some time to boot up.	
	Reboot Cancel

Note: System Reboot. System Reset.
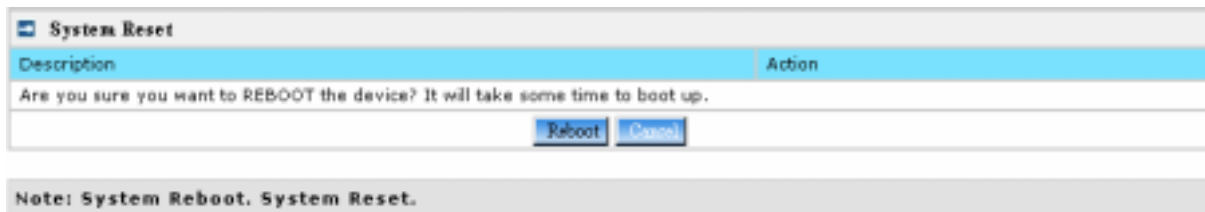
Figure 60 – Reboot the device

To reset device to factory defaults, click **Reset** on *Figure 48* and then the below appears to make sure:

System Reset	
Description	**Action**
Are you sure you want to RESET the device? It will take some time to boot up.	
	Reset Cancel

Note: System Reboot. System Reset.
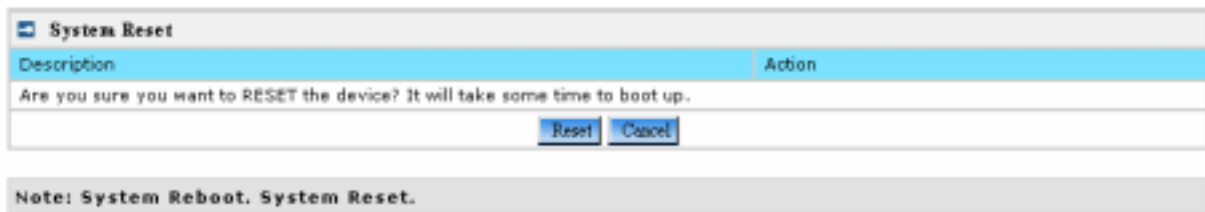
Figure 61 – Reset the device

> Please note that all settings including the administrator settings will be set back to the factory default when **Reset** is selected.

System | Upgrade

> Check for new product updates at the Gemtek Systems website:
> http://www.gemtek-systems.com

Upload – Update your device firmware.

Figure 62 – Firmware Upgrade

Click the **Upload** and then the follow appears. Specify the full path to the new firmware image and click the **Upload** button:

Figure 63 – Firmware Upgrade

To flash the uploaded firmware image to upgrade the firmware is done by click the **Upgrade** button.

Please make sure the firmware is correct for P-780. Otherwise the upgrade will be failed.

Figure 64 – Device Statistics

Do not switch off and do not disconnect the P-780 from the power supply during the firmware update process because the device could be damaged. It is best to use the Ethernet connection (not wireless) for the firmware update process.

▪

Appendix

A) Specification

Wireless	
Standard	IEEE 802.11b(DSSS), IEEE 802.11g(OFDM) and IEEE 802.11a(OFDM)
Data Rate	802.11a: 54,48,36,24,18,12,9,6Mbps;802.11g: 54,48,36,24,12,9,6,11,5,5,2,1Mbps (auto fall back)
Transmit Power (adjustable RF power)	Max. 17 dBm ± 1.5dBm @6~24Mbps Max. 13 dBm ± 1.5dBm @54Mbps (Maximum power will vary by channel, rate and regulatory domain)
Antennas	two N type connectors
Encryption	WPA TKIP and CCMP-AES , WEP64, WEP128
Bridge	Up to 20 bridge links
Interface	
LAN	10/100Mb Ethernet, auto sensing, RJ-45
WLAN1	N-type Connector
WLAN2	N-type Connector
Management	
Interfaces	HTTPs, Secure Telnet(SSHv2), SNMP
Software Update	Remote software update via HTTPs
Reset	Remote restore factory default
Physical Specification	
Dimension	180 mm x 160 mm x 58 mm
Weight	1.2kg

Environment Specification		
	Temperature	Humidity
Operating	-40 to 70°C	95%, non-condensing

Power Supply	
POE	48V, IEEE802.3af-2003 compliance
LEDs	
3 LEDs	LAN, WLAN1, WLAN2

Warranty
1 years

Package Contents	
▪ P-780 Dual-Band Outdoor Access Point	▪ Mounting Kit including SCREW
▪ Printed warranty note, release note, warning card	▪ CD with P-780 Firmware , Kickstart Utility and User manual(*.pdf)
▪ Omni Dual-Band Antenna(A-807) * 2	▪ Waterproof tape
▪ Waterproof RJ45 Straight Plug	▪

Related Products

Controllers:	**G-6000/G-4200** Public Access Controller
Access Points:	**P-520** 54Mb Operator Access Point **P-560** 54Mb Hotspot-in-a-Box
Client Adapters:	**T-511** 54Mb High Gain Smart Ethernet Client (2.4 GHz)

B) Factory Defaults for the P-780

General Configuration Settings	
Administrator Username	admin
Administrator Password	admin01
Get Community	Public
Set Community	Private

Network Configuration Settings	
IP address	(static IP) 192.168.2.2
Subnet mask	255.255.255.0
Gateway	0.0.0.0

Wireless Configuration Settings	

RF Card 1(WLAN1)	
Default Mode	11g Access Point
Regulatory Domain	World
SSID	P-780
Default channel	11
RTS Threshold	2347 bytes
Authentication Type	Open System
Encryption	Off

RF Card 2(WLAN2)	
Default Mode	11a Access Point
Regulatory Domain	World
SSID	P-780
Default channel	60
RTS Threshold	2347 bytes
Authentication Type	Open System
Encryption	Off

C) Regulatory Domain/Channels/Power

Channels and Maximum output power for the P-780 11g radio:

Channels Identifiers	Frequency in MHz	USA, Canada (FCC)	European Union (CE/ETSI)	WORLD (CE&FCC)	Japan (TELEC)
1	2412	•	•	•	•
2	2417	•	•	•	•
3	2422	•	•	•	•
4	2427	•	•	•	•
5	2432	•	•	•	•
6	2437	•	•	•	•
7	2442	•	•	•	•
8	2447	•	•	•	•

9	2452	•	•	•	•
10	2457	•	•	•	•
11	2462	•	•	•	•
12	2467	—	•	—	•
13	2472	—	•	—	•
14	2484	—	—	—	—
Maximum output Power		16dBm	14dBm	14dBm	14dBm

Channels and Maximum power for the P-780 11a radio:

Channels Identifiers	Frequency in MHz	USA, Canada (FCC)	European Union (CE/ETSI)	WORLD (CE/FCC)	Japan (TELEC)
U-NII lower band (5150 – 5250 MHz)					
34	5170	—	—	—	•
36	5180	•	•	•	—
38	5190	—	—	—	•
40	5200	•	•	•	—
42	5210	—	—	—	•
44	5220	•	•	•	—
46	5230	—	—	—	•
48	5240	•	•	•	—
Maximum Output Power		12 dBm	17 dBm	15 dBm	15 dBm
U-NII middle band (5250 – 5350 MHz)					
52	5260	•	•	•	—
56	5280	•	•	•	—
60	5300	•	•	•	—
64	5320	•	•	•	—
Maximum Output Power		12 dBm	17 dBm	17 dBm	—
U-NII upper band (5725 – 5875 MHz)					
149	5745	•	—	—	—
153	5765	•	—	—	—
157	5785	•	—	—	—
161	5805	•	—	—	—
165	5825	—	—	—	—
Maximum Output Power		14 dBm	17 dBm	17 dBm	—

F) Location ID and ISO Country Codes

This list states the **country names** (official short names in English) in alphabetical order as given in ISO 3166-1 **and** the corresponding **ISO 3166-1-alpha-2 code elements**.

It lists 239 official short names and code elements.

Location ID	Country	Location ID	Country
AF	Afghanistan	LI	Liechtenstein
AL	Albania	LT	Lithuania
DZ	Algeria	LU	Luxembourg
AS	American Samoa	MO	Macao
AD	Andorra	MK	Macedonia, the former Yugoslav republic of
AO	Angola	MG	Madagascar
AI	Anguilla	MW	Malawi
AQ	Antarctica	MY	Malaysia
AG	Antigua and Barbuda	MV	Maldives
AR	Argentina	ML	Mali
AM	Armenia	MT	Malta
AW	Aruba	MH	Marshall islands
AU	Australia	MQ	Martinique
AT	Austria	MR	Mauritania
AZ	Azerbaijan	MU	Mauritius
BS	Bahamas	YT	Mayotte
BH	Bahrain	MX	Mexico
BD	Bangladesh	FM	Micronesia, federated states of
BB	Barbados	MD	Moldova, republic of
BY	Belarus	MC	Monaco
BE	Belgium	MN	Mongolia
BZ	Belize	MS	Montserrat
BJ	Benin	MA	Morocco
BM	Bermuda	MZ	Mozambique
BT	Bhutan	MM	Myanmar
BO	Bolivia	NA	Namibia
BA	Bosnia and Herzegovina	NR	Nauru
BW	Botswana	NP	Nepal
BV	Bouvet island	NL	Netherlands
BR	Brazil	AN	Netherlands Antilles
IO	British Indian ocean territory	NC	New Caledonia
BN	Brunei Darussalam	NZ	New Zealand
BG	Bulgaria	NI	Nicaragua
BF	Burkina Faso	NE	Niger

BI	Burundi	NG	Nigeria
KH	Cambodia	NU	Niue
CM	Cameroon	NF	Norfolk island
CA	Canada	MP	Northern Mariana islands
CV	Cape Verde	NO	Norway
KY	Cayman islands	OM	Oman
CF	Central African republic	PK	Pakistan
TD	Chad	PW	Palau
CL	Chile	PS	Palestinian territory, occupied
CN	China	PA	Panama
CX	Christmas island	PG	Papua new guinea
CC	Cocos (keeling) islands	PY	Paraguay
CO	Colombia	PE	Peru
KM	Comoros	PH	Philippines
CG	Congo	PN	Pitcairn
CD	Congo, the democratic republic of the	PL	Poland
CK	Cook islands	PT	Portugal
CR	Costa Rica	PR	Puerto Rico
CI	Côte d'ivoire	QA	Qatar
HR	Croatia	RE	Réunion
CU	Cuba	RO	Romania
CY	Cyprus	RU	Russian federation
CZ	Czech republic	RW	Rwanda
DK	Denmark	SH	Saint Helena
DJ	Djibouti	KN	Saint Kitts and Nevis
DM	Dominica	LC	Saint Lucia
DO	Dominican republic	PM	Saint Pierre and Miquelon
EC	Ecuador	VC	Saint Vincent and the grenadines
EG	Egypt	WS	Samoa
SV	El Salvador	SM	San Marino
GQ	Equatorial guinea	ST	Sao tome and Principe
ER	Eritrea	SA	Saudi Arabia
EE	Estonia	SN	Senegal
ET	Ethiopia	SC	Seychelles
FK	Falkland islands (malvinas)	SL	Sierra Leone
FO	Faroe islands	SG	Singapore
FJ	Fiji	SK	Slovakia
FI	Finland	SI	Slovenia
FR	France	SB	Solomon islands
GF	French Guiana	SO	Somalia
PF	French Polynesia	ZA	South Africa

TF	French southern territories	GS	South Georgia and the south sandwich islands
GA	Gabon	ES	Spain
GM	Gambia	LK	Sri Lanka
GE	Georgia	SD	Sudan
DE	Germany	SR	Suriname
GH	Ghana	SJ	Svalbard and Jan Mayan
GI	Gibraltar	SZ	Swaziland
GR	Greece	SE	Sweden
GL	Greenland	CH	Switzerland
GD	Grenada	SY	Syrian Arab republic
GP	Guadeloupe	TW	Taiwan, province of china
GU	Guam	TJ	Tajikistan
GT	Guatemala	TZ	Tanzania, united republic of
GN	Guinea	TH	Thailand
GW	Guinea-Bissau	TL	Timor-leste
GY	Guyana	TG	Togo
HT	Haiti	TK	Tokelau
HM	Heard island and McDonald islands	TO	Tonga
VA	Holy see (Vatican city state)	TT	Trinidad and Tobago
HN	Honduras	TN	Tunisia
HK	Hong Kong	TR	Turkey
HU	Hungary	TM	Turkmenistan
IS	Iceland	TC	Turks and Caicos islands
IN	India	TV	Tuvalu
ID	Indonesia	UG	Uganda
IR	Iran, Islamic republic of	UA	Ukraine
IQ	Iraq	AE	United Arab emirates
IE	Ireland	GB	United kingdom
IL	Israel	US	United states
IT	Italy	UM	United states minor outlying islands
JM	Jamaica	UY	Uruguay
JP	Japan	UZ	Uzbekistan
JO	Jordan	VU	Vanuatu
KZ	Kazakhstan		Vatican city state see holy see
KE	Kenya	VE	Venezuela
KI	Kiribati	VN	Viet nam
KP	Korea, democratic people's republic of	VG	Virgin islands, British
KR	Korea, republic of	VI	Virgin islands, u.s.
KW	Kuwait	WF	Wallis and Futuna
KG	Kyrgyzstan	EH	Western Sahara

LA	Lao people's democratic republic	YE	Yemen
LV	Latvia	YU	Yugoslavia
LB	Lebanon		Zaire see Congo, the democratic republic of the
LS	Lesotho	ZM	Zambia
LR	Liberia	ZW	Zimbabwe
LY	Libyan Arab Jamahiriya		

Professional installation instruction

1. Installation personal
   This product is designed for specific application and needs to be installed by a qualified personal who has RF and related rule knowledge. The general user shall not attempt to install or change the setting.

2. Installation location
   The product shall be installed at a location where the radiating antenna can be kept 20 cm from nearby person in normal operation condition to meet regulatory RF exposure requirement.

3. External   antenna,
   Use only the antennas which have been approved by Gemtek. The non-approved antenna(s) may produce unwanted spurious or excessive RF transmitting power which may lead to the violation of FCC limit and is prohibited.

4. Installation procedure
   Please refer to user's manual for the detail.

5. Warning
   Please carefully select the installation position and make sure that the final output power does not exceed the limit set force in US Rule CFR 47 part 15 section 15.247. and 15.407 The violation of the rule could lead to serious federal penalty.